Guidelines for Reporting Breaches

Purpose:

Protecting the privacy and security of personally identifiable information (PII) and protected health information (PHI) is the responsibility of all DHA Directorates, Divisions, and Special Staff elements, to include the TRICARE Regional Offices, TRICARE Area Offices, and all other organizational entities within DHA. All of DHA must adhere to the reporting and notification requirements set forth in the DoDD 5400.11, "Department of Defense Privacy Program," October 29, 2014, Office of the Secretary of Defense Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2009; DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, or its successor issuance; and DoD 6025.18-R, "Department of Defense Health Information Privacy Regulation," January 24, 2003, or its successor issuance.

Definition:

DoDD 5400.11 defines "lost, stolen or compromised information," otherwise termed a breach, as follows:

"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

The DHA Privacy Office will determine whether a breach meets the requirements of reporting to the Department of Health and Human Services (HHS).

Guidance:

This document outlines the DoD Reporting and Notification Requirements for breaches:

1. Notify your Supervisor/Director (immediately, upon discovery)
2. *Notify the United States Computer Emergency Readiness Team (within 1 hour only if the breach is confirmed as cyber-security related, e.g., not a paper breach))*
    - If breach is internal to DHA, report to the DHA Privacy Office within 1 hour.
3. Notify the Agency Privacy Officer/Senior Representative for the Service/Senior Component for Privacy (within 24 hours)
    - If breach is external to DHA, report to the DHA Privacy Office within 24 hours at dha.ncr.pcl.mbx.dha-privacy-officer@mail.mil or (703) 681-7500 and the Contracting Officer within 24 hours.
    - The DoD breach reporting form (DD Form 2959) is available on the DHA Privacy Office website at: http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI
4. Notify the Defense Privacy and Civil Liberties Division and Component Head (within 48 hours) (completed by the DHA Privacy Office)
5. Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if required by the DHA Privacy Office
6. Notify law enforcement authorities, if necessary
7. Notify issuing banks if government issued credit cards are involved

If PHI is involved, please refer to DHA Privacy Office guidance for additional breach reporting and notification actions as required by the HHS Final Omnibus Rule and Title 45, CFR, Parts 160 and 164.

Breaches often occur when PII or PHI is mishandled. Examples of these types of breaches may include, but are not limited to:

- Misdirected fax documents that reach anyone other than the intended recipient
- Failing to properly secure documents when mailing or transporting
- Lost or stolen removable media devices (e.g., laptops, thumb drives, compact discs)
- Transmission of unsecured e-mails and unencrypted files
- Unauthorized access to computer systems
- Inappropriate disposal of documents
- Inadvertent posting on the internet